PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-333775

(43)Date of publication of application : 17.12.1993

(51)Int.Cl. G09C 1/00
G06F 15/16

(21)Application number : 04-142770

(22)Date of filing : 03.06.1992

(71)Applicant : TOSHIBA CORP

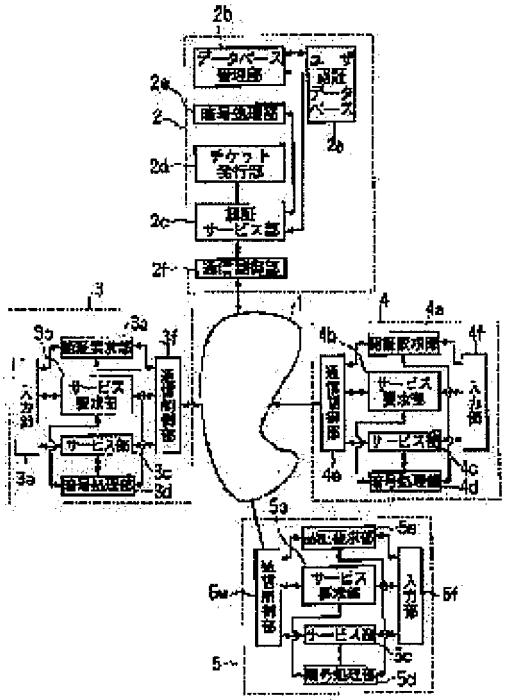
(72)Inventor : SAWA KIMIO
NUKUI HARUMI

(54) USER AUTHENTICATION SYSTEM

(57)Abstract:

PURPOSE: To provide the user authentication system which can be improved in safety and operability than heretofore.

CONSTITUTION: A computer system 2 is equipped with a user authentication database 2a, a database control part 2b which controls the user authentication database 2a, a certifying service part 2c which offers authentication service, a ticket issue part 2d which issues a ticket having a time limit, a ciphering process part 2e which ciphers and composes information, and a communication control part 2f which transmits and receives information through a communication medium 1. Computer systems 3-5 are equipped with certification request parts 3a-5a which sends certification requests to the computer system 2, service request parts 3b-5b which sends service requests to other computer systems, service parts 3c-5c which offer the service, ciphering process parts 3d-5d, input parts 3e-5e, and communication control parts 3f-5f.



LEGAL STATUS

[Date of request for examination] 12.01.1999

[Date of sending the examiner's decision of 10.04.2001

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the user authentication system in the security system of the network system which consists of two or more computer systems organically connected through communication media.
[0002]
[Description of the Prior Art] In recent years, two or more computer systems are connected through the communication media of arbitration, and the network system which made the file and CPU of these computer systems available mutually is developed.
[0003] There is much what consisted of such network systems so that a user might be attested in the case of the use initiation procedure of a computer system and the initiation procedure which starts various services for security etc. Conventionally, such a user's authentication judges authorization or refusal of use each time based on the user information which the computer system concerned itself manages [the computer system used as the candidate for use].
[0004] Therefore, when using service of the computer system of an and also [authentication is the need], from the computer system which performed alter operation, the information on a user name, a password, etc. which the user entered passes along communication media, and is transmitted to the computer system used as the candidate for use.
[0005]
[Problem(s) to be Solved by the Invention] As mentioned above, the computer system used as the candidate for use is carrying out a user's authentication accompanying the use initiation procedure of a computer system etc. conventionally based on the user information which the computer system concerned itself manages.
[0006] However, in such a system, since the communication-media top was flowed in the form which a user's information (a user name, password, etc.) can decipher for a third person, there was a problem of not being desirable on insurance. Moreover, when the user information managed for every computer on a network differed, the user had to change the user identifier (password) etc. by computer for use, and also had the problem that operability was spoiled.
[0007] This invention coped with this conventional situation, was made, and tends to offer the user authentication system which can aim at improvement in safety, and improvement in operability compared with the former.
[0008]
[Means for Solving the Problem] Namely, two or more computer systems set this invention to the user authentication system of the network system which was connected through communication media and was mutually constituted available in the file and CPU of these computer systems. It responds to said network system from said each computer system at a user authentication demand. When a storage means to store User Information is searched, it judges whether the user is registered or not and the user is registered While establishing the computer system for authentication which enciphers and returns the

ticket which proves a user's justification with the time limit, and the password stored in said storage means It is characterized by establishing a cipher-processing means to encipher exchange of said User Information on said communication media to said each computer system.
[0009]
[Function] According to the user authentication system of this invention of the above-mentioned configuration, since unitary management of User Information in a network is carried out according to the computer system for authentication, a password etc. can be unified and improvement in operability can be aimed at compared with the former.
[0010] Moreover, to communication media, since the time limit is attached, the ticket which User Information does not flow in the form which can be deciphered for a third person, and is further used for authentication can also reduce possibility of being unfairly used for a third person, and to them, it can aim at improvement in safety compared with the former.
[0011]
[Example] Hereafter, one example of this invention is explained with reference to a drawing.
[0012] Drawing 1 shows the configuration of one example of this invention. In this drawing, 1 is communication media and two or more computer systems 2, 3, 4, and 5 are connected through these communication media 1.
[0013] A computer system 2 among each above-mentioned computer system User authentication database 2a which is the authentication server which carries out package management of User Information on a network, and stores User Information, Data base manager 2b which manages this user authentication database 2a, Authentication courtesy counter 2c which offers authentication service in response to the authentication demand from other computer systems 3, 4, and 5, It is a ticket used as the radical which judges a user's use permission at the time of service, and has 2d of ticket issue sections which publish the ticket to which the time limit was attached, cipher-processing section 2e which performs informational encryption and informational ****, and 2f of communications control sections which transmit and receive information through communication media 1.
[0014] Moreover, the authentication demand sections 3a, 4a, and 5a which computer systems 3, 4, and 5 are computers which a user generally uses, and perform an authentication demand to a computer system 2, The service request sections 3b, 4b, and 5b which perform a service request to other computer systems, It has the courtesy counters 3c, 4c, and 5c which perform service, the cipher-processing sections 3d, 4d, and 5d which perform cipher processing mentioned above, the input sections 3e, 4e, and 5e for a user to input, and the communications control sections 3f, 4f, and 5f which transmit and receive information through communication media 1.
[0015] Here, procedure until a user starts use and starts use of service of a computer system 4 in a computer system 3 is made into an example, and an authentication procedure is explained.
[0016] First, the user authentication procedure of the initial authentication at the time of use initiation of a computer system 3 is explained. As shown in the flow chart of drawing 2 , a user inputs a user name first to input section 3e to authentication demand section 3a of a computer system 3 (100).
[0017] Authentication demand section 3a requires the enciphered password which is registered into the computer system (authentication server) 2 in this inputted user name through communication media 1 by 3f of communications control sections at delivery, a user's initial ticket, and user authentication database 2a (101).
[0018] In a computer system 2, the user name which received by 2f of communications control sections is inputted into authentication courtesy counter 2c, authentication courtesy counter 2c sends a user name to data base manager 2b, and this user name confirms whether register with user authentication database 2a (102).
[0019] And if the user name is registered, by 2d of ticket issue sections, the initial ticket to which the time limit of predetermined time (for example, several hours thru/or about ten hours) was attached will be created (103), and this initial ticket and the password registered into user authentication database 2a corresponding to the user name will be enciphered in cipher-processing section 2e (104). Here, a time limit is imposed on an initial ticket for preventing the unauthorized use by the third person. That is, if

there is no time limit in an initial ticket, after a valid user's receiving authentication, publishing an initial ticket and using the computer system concerned, it is because a third person may use the computer system concerned improperly with this initial ticket.
[0020] On the other hand, when the user is not registered into user authentication database 2a, it supposes that authentication is impossible (105) and these results are returned to a computer system 3 through 2f of communications control sections (106).
[0021] In a computer system 3, the result of 3f smell lever of communications control sections is received, and it inputs into authentication demand section 3a. In authentication demand section 3a, if the input of a password is demanded from a user from input section 3e and a user enters a password (107), in 3d of cipher-processing sections, the transmitting contents from a computer system 2 will be decoded (108), and it will judge whether these passwords are in agreement (109). Here, if a password is in agreement, a computer system 3 will become available and an initial ticket will become effective between the time limit. Moreover, using becomes impossible if a password is not in agreement.
[0022] In addition, the protocol of the user authentication at the time of the above-mentioned beginning of using is shown in drawing 5 . In this drawing, the computer system 2 whose C is a computer system 3 and whose AS is an authentication server is shown.
[0023] Next, a user explains the case where service of a computer system 3 to the computer system 4 is used.
[0024] As shown in drawing 3 , when a user inputs the purport which wants to use service of a computer system 4 for service request section 3b from input section 3e, it investigates whether service request section 3b has a certificate for service (service ticket) (200) and there is almost no service ticket, a service ticket is required from a computer system 2 (201).
[0025] And when there is a service ticket, next, an initial ticket investigates ****** within an expiration date (202), (when there is no service ticket, after receiving a service ticket from a computer system 2), if it is within an expiration date, a service ticket will be enciphered in 3d of cipher-processing sections (203), this enciphered service ticket will be sent to a computer system 4 from 3f of communications control sections, and a service request will be performed (204).
[0026] In a computer system 4, in communications control section 4e, the above-mentioned service request is received and this service request is inputted into courtesy counter 4c. In courtesy counter 4c, the service ticket sent in 4d of cipher-processing sections is decoded (205), and it checks whether you are a right user (206). And when it is a right user, the purport which receives service is returned, service is started, and when it is not a right user, the purport which refuses service is returned.
[0027] In addition, the protocol of the user authentication at the time of the above-mentioned service is shown in drawing 6 . In this drawing, the computer system 2 whose C is a computer system 3 and whose AS is an authentication server, and S show the computer system 4 which gives its service.
[0028] Next, processing of the service ticket demand in step 201 mentioned above and issue is explained.
[0029] When it does not have a service ticket, as shown in drawing 4 , by the computer system 3, in 3d of cipher-processing sections, an initial ticket and the computer system name (computer system 4) to be used are enciphered first (300), these are sent to a computer system 2 from 3f of communications control sections, and issue of a service ticket is required (301).
[0030] In a computer system 2, the demand of 2f smell lever of communications control sections is received, and this demand is inputted into authentication courtesy counter 2c. In authentication courtesy counter 2c, the data sent by cipher-processing section 2e are decoded (302), and an initial ticket checks the right or no (isn't it time-out?) (303).
[0031] And a service ticket is created in 2d of ticket issue sections (304), and an initial ticket enciphers this service ticket by cipher-processing section 2e (305), and returns a right case to a computer system 3 from 2f of communications control sections. Moreover, that is returned to a computer system 3 when an initial ticket is time-out (306).
[0032] In a computer system 3, 3f of communications control sections receives a service ticket, and this service ticket is decoded and stored by 3d of cipher-processing sections (307).

[0033] Thus, since unitary management of User Information in a network is carried out according to the computer system 2 which is an authentication server according to this example, a password etc. can be unified and improvement in operability can be aimed at compared with the former. Moreover, to communication media 1, since the time limit is attached, the initial ticket which User Information does not flow in the form which can be deciphered for a third person, and is further used for authentication can also reduce possibility of being unfairly used for a third person, and to them, it can aim at improvement in safety compared with the former.
[0034]
[Effect of the Invention] As explained above, according to the user authentication system of this invention, compared with the former, improvement in safety and improvement in operability can be aimed at.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In the user authentication system of the network system which two or more computer systems were connected through communication media, and was mutually constituted available in the file and CPU of these computer systems It responds to said network system from said each computer system at a user authentication demand. When a storage means to store User Information is searched, it judges whether the user is registered or not and the user is registered While establishing the computer system for authentication which enciphers and returns the ticket which proves a user's justification with the time limit, and the password stored in said storage means The user authentication system characterized by establishing a cipher-processing means to encipher exchange of said User Information on said communication media to said each computer system.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Industrial Application] This invention relates to the user authentication system in the security system of the network system which consists of two or more computer systems organically connected through communication media.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art] In recent years, two or more computer systems are connected through the communication media of arbitration, and the network system which made the file and CPU of these computer systems available mutually is developed.
[0003] There is much what consisted of such network systems so that a user might be attested in the case of the use initiation procedure of a computer system and the initiation procedure which starts various services for security etc. Conventionally, such a user's authentication judges authorization or refusal of use each time based on the user information which the computer system itself [concerned] manages [the computer system used as the candidate for use].
[0004] Therefore, when using service of the computer system of an and also [authentication is the need], from the computer system which performed alter operation, the information on a user name, a password, etc. which the user entered passes along communication media, and is transmitted to the computer system used as the candidate for use.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] As explained above, according to the user authentication system of this invention, compared with the former, improvement in safety and improvement in operability can be aimed at.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] As mentioned above, the computer system used as the candidate for use is carrying out a user's authentication accompanying the use initiation procedure of a computer system etc. conventionally based on the user information which the computer system concerned itself manages.
[0006] However, in such a system, since the communication-media top was flowed in the form which a user's information (a user name, password, etc.) can decipher for a third person, there was a problem of not being desirable on insurance. Moreover, when the user information managed for every computer on a network differed, the user had to change the user identifier (password) etc. by computer for use, and also had the problem that operability was spoiled.
[0007] This invention coped with this conventional situation, was made, and tends to offer the user authentication system which can aim at improvement in safety, and improvement in operability compared with the former.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] Namely, two or more computer systems set this invention to the user authentication system of the network system which was connected through communication media and was mutually constituted available in the file and CPU of these computer systems. It responds to said network system from said each computer system at a user authentication demand. When a storage means to store User Information is searched, it judges whether the user is registered or not and the user is registered While establishing the computer system for authentication which enciphers and returns the ticket which proves a user's justification with the time limit, and the password stored in said storage means It is characterized by establishing a cipher-processing means to encipher exchange of said User Information on said communication media to said each computer system.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

OPERATION

[Function] According to the user authentication system of this invention of the above-mentioned configuration, since unitary management of User Information in a network is carried out according to the computer system for authentication, a password etc. can be unified and improvement in operability can be aimed at compared with the former.
[0010] Moreover, to communication media, since the time limit is attached, the ticket which User Information does not flow in the form which can be deciphered for a third person, and is further used for authentication can also reduce possibility of being unfairly used for a third person, and to them, it can aim at improvement in safety compared with the former.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EXAMPLE

[Example] Hereafter, one example of this invention is explained with reference to a drawing.
[0012] Drawing 1 shows the configuration of one example of this invention. In this drawing, 1 is communication media and two or more computer systems 2, 3, 4, and 5 are connected through these communication media 1.
[0013] A computer system 2 among each above-mentioned computer system User authentication database 2a which is the authentication server which carries out package management of User Information on a network, and stores User Information, Data base manager 2b which manages this user authentication database 2a, Authentication courtesy counter 2c which offers authentication service in response to the authentication demand from other computer systems 3, 4, and 5, It is a ticket used as the radical which judges a user's use permission at the time of service, and has 2d of ticket issue sections which publish the ticket to which the time limit was attached, cipher-processing section 2e which performs informational encryption and informational ****, and 2f of communications control sections which transmit and receive information through communication media 1.
[0014] Moreover, the authentication demand sections 3a, 4a, and 5a which computer systems 3, 4, and 5 are computers which a user generally uses, and perform an authentication demand to a computer system 2, The service request sections 3b, 4b, and 5b which perform a service request to other computer systems, It has the courtesy counters 3c, 4c, and 5c which perform service, the cipher-processing sections 3d, 4d, and 5d which perform cipher processing mentioned above, the input sections 3e, 4e, and 5e for a user to input, and the communications control sections 3f, 4f, and 5f which transmit and receive information through communication media 1.
[0015] Here, procedure until a user starts use and starts use of service of a computer system 4 in a computer system 3 is made into an example, and an authentication procedure is explained.
[0016] First, the user authentication procedure of the initial authentication at the time of use initiation of a computer system 3 is explained. As shown in the flow chart of drawing 2 , a user inputs a user name first to input section 3e to authentication demand section 3a of a computer system 3 (100).
[0017] Authentication demand section 3a requires the enciphered password which is registered into the computer system (authentication server) 2 in this inputted user name through communication media 1 by 3f of communications control sections at delivery, a user's initial ticket, and user authentication database 2a (101).
[0018] In a computer system 2, the user name which received by 2f of communications control sections is inputted into authentication courtesy counter 2c, authentication courtesy counter 2c sends a user name to data base manager 2b, and this user name confirms whether register with user authentication database 2a (102).
[0019] And if the user name is registered, by 2d of ticket issue sections, the initial ticket to which the time limit of predetermined time (for example, several hours thru/or about ten hours) was attached will be created (103), and this initial ticket and the password registered into user authentication database 2a corresponding to the user name will be enciphered in cipher-processing section 2e (104). Here, a time limit is imposed on an initial ticket for preventing the unauthorized use by the third person. That is, if

there is no time limit in an initial ticket, after a valid user's receiving authentication, publishing an initial ticket and using the computer system concerned, it is because a third person may use the computer system concerned improperly with this initial ticket.
[0020] On the other hand, when the user is not registered into user authentication database 2a, it supposes that authentication is impossible (105) and these results are returned to a computer system 3 through 2f of communications control sections (106).
[0021] In a computer system 3, the result of 3f smell lever of communications control sections is received, and it inputs into authentication demand section 3a. In authentication demand section 3a, if the input of a password is demanded from a user from input section 3e and a user enters a password (107), in 3d of cipher-processing sections, the transmitting contents from a computer system 2 will be decoded (108), and it will judge whether these passwords are in agreement (109). Here, if a password is in agreement, a computer system 3 will become available and an initial ticket will become effective between the time limit. Moreover, using becomes impossible if a password is not in agreement.
[0022] In addition, the protocol of the user authentication at the time of the above-mentioned beginning of using is shown in drawing 5 . In this drawing, the computer system 2 whose C is a computer system 3 and whose AS is an authentication server is shown.
[0023] Next, a user explains the case where service of a computer system 3 to the computer system 4 is used.
[0024] As shown in drawing 3 , when a user inputs the purport which wants to use service of a computer system 4 for service request section 3b from input section 3e, it investigates whether service request section 3b has a certificate for service (service ticket) (200) and there is almost no service ticket, a service ticket is required from a computer system 2 (201).
[0025] And when there is a service ticket, next, an initial ticket investigates ****** within an expiration date (202), (when there is no service ticket, after receiving a service ticket from a computer system 2), if it is within an expiration date, a service ticket will be enciphered in 3d of cipher-processing sections (203), this enciphered service ticket will be sent to a computer system 4 from 3f of communications control sections, and a service request will be performed (204).
[0026] In a computer system 4, in communications control section 4e, the above-mentioned service request is received and this service request is inputted into courtesy counter 4c. In courtesy counter 4c, the service ticket sent in 4d of cipher-processing sections is decoded (205), and it checks whether you are a right user (206). And when it is a right user, the purport which receives service is returned, service is started, and when it is not a right user, the purport which refuses service is returned.
[0027] In addition, the protocol of the user authentication at the time of the above-mentioned service is shown in drawing 6 . In this drawing, the computer system 2 whose C is a computer system 3 and whose AS is an authentication server, and S show the computer system 4 which gives its service.
[0028] Next, processing of the service ticket demand in step 201 mentioned above and issue is explained.
[0029] When it does not have a service ticket, as shown in drawing 4 , by the computer system 3, in 3d of cipher-processing sections, an initial ticket and the computer system name (computer system 4) to be used are enciphered first (300), these are sent to a computer system 2 from 3f of communications control sections, and issue of a service ticket is required (301).
[0030] In a computer system 2, the demand of 2f smell lever of communications control sections is received, and this demand is inputted into authentication courtesy counter 2c. In authentication courtesy counter 2c, the data sent by cipher-processing section 2e are decoded (302), and an initial ticket checks the right or no (isn't it time-out?) (303).
[0031] And a service ticket is created in 2d of ticket issue sections (304), and an initial ticket enciphers this service ticket by cipher-processing section 2e (305), and returns a right case to a computer system 3 from 2f of communications control sections. Moreover, that is returned to a computer system 3 when an initial ticket is time-out (306).
[0032] In a computer system 3, 3f of communications control sections receives a service ticket, and this service ticket is decoded and stored by 3d of cipher-processing sections (307).

[0033] Thus, since unitary management of User Information in a network is carried out according to the computer system 2 which is an authentication server according to this example, a password etc. can be unified and improvement in operability can be aimed at compared with the former. Moreover, to communication media 1, since the time limit is attached, the initial ticket which User Information does not flow in the form which can be deciphered for a third person, and is further used for authentication can also reduce possibility of being unfairly used for a third person, and to them, it can aim at improvement in safety compared with the former.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] Drawing showing the configuration of one example of this invention.
[Drawing 2] Drawing showing the procedure of the user authentication at the time of the beginning of using in one example of this invention.
[Drawing 3] Drawing showing the procedure of the user authentication at the time of the service in one example of this invention.
[Drawing 4] Drawing showing the procedure of the service ticket issue in one example of this invention.

[Drawing 5] Drawing showing the protocol of the user authentication at the time of the beginning of using.
[Drawing 6] Drawing showing the protocol of the user authentication at the time of service.
[Description of Notations]
1 Communication Media
2 Computer System (for Authentication)
2a User authentication database
2b Data base manager
2c Authentication courtesy counter
2d Ticket issue section
2e Cipher-processing section
2f Communications control section
3, 4, 5 Computer system
3d, 4d, 5d Cipher-processing section

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平5－333775

(43)公開日　平成５年(1993)12月17日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　1/00		9194－5L		
Ｇ０６Ｆ　15/16	３７０　Ｚ	8840－5L		

審査請求　未請求　請求項の数１(全　８　頁)

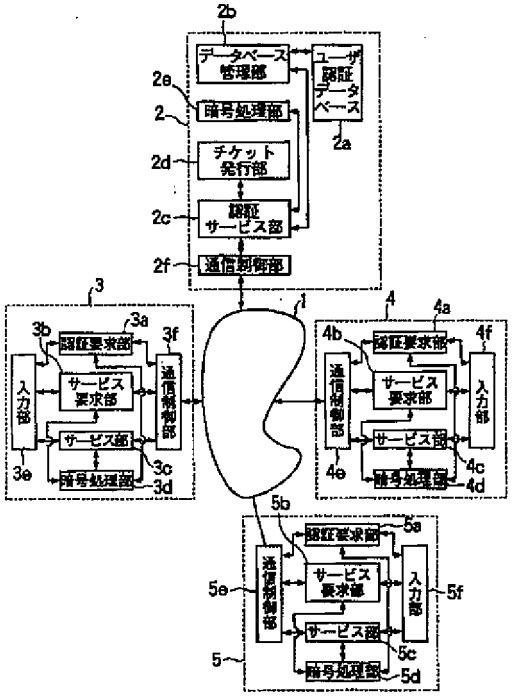
(21)出願番号　特願平4－142770

(22)出願日　平成４年(1992)６月３日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　佐波　公夫
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内
(72)発明者　賀井　春美
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内
(74)代理人　弁理士　須山　佐一

(54)【発明の名称】　ユーザ認証システム

(57)【要約】
【目的】　従来に較べて安全性の向上と、操作性の向上を図ることのできるユーザ認証システムを提供する。
【構成】　コンピュータシステム２は、ユーザ認証データベース２ａと、ユーザ認証データベース２ａを管理するデータベース管理部２ｂと、認証サービスを行う認証サービス部２ｃと、時間制限の付いたチケットを発行するチケット発行部２ｄと、情報の暗号化および復合を行う暗号処理部２ｅと、通信媒体１を介して情報の送受信を行う通信制御部２ｆとを備えている。コンピュータシステム３～５は、コンピュータシステム２に対して認証要求を行う認証要求部３ａ～５ａと、他のコンピュータシステムに対してサービス要求を行うサービス要求部３ｂ～５ｂと、サービスを実行するサービス部３ｃ～５ｃと、暗号処理部３ｄ～５ｄと、入力部３ｅ～５ｅと、通信制御部３ｆ～５ｆとを備えている。



1

【特許請求の範囲】

【請求項１】　複数のコンピュータシステムが通信媒体を介して接続され、これらのコンピュータシステムのファイルやＣＰＵを相互に利用可能に構成されたネットワークシステムのユーザ認証システムにおいて、

前記ネットワークシステムに、前記各コンピュータシステムからのユーザ認証要求に応じて、ユーザ情報を格納する記憶手段を検索してユーザが登録されているか否かを判定し、ユーザが登録されている場合は、ユーザの正当性を制限時間付きで証明するチケットと前記記憶手段に格納されたパスワードとを暗号化して返送する認証用のコンピュータシステムを設けるとともに、

前記各コンピュータシステムに、前記通信媒体上での前記ユーザ情報の交換を暗号化する暗号処理手段を設けたことを特徴とするユーザ認証システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、通信媒体を介して有機的に接続された複数のコンピュータシステムから構成されるネットワークシステムのセキュリティシステムにおけるユーザ認証システムに関する。

【０００２】

【従来の技術】近年、任意の通信媒体を介して複数のコンピュータシステムを接続し、これらのコンピュータシステムのファイルやＣＰＵを相互に利用可能としたネットワークシステムが開発されている。

【０００３】このようなネットワークシステムでは、セキュリティ等のため、コンピュータシステムの利用開始手続や、各種サービスを開始する開始手続の際に、ユーザの認証を行うよう構成されたものが多い。従来、このようなユーザの認証は、利用対象となるコンピュータシステムが、当該コンピュータシステム自身が管理する利用者情報を基に、利用の許可または拒否をその都度判断している。

【０００４】したがって、認証が必要な他のコンピュータシステムのサービスを利用する場合、利用者が入力したユーザ名やパスワード等の情報は、入力操作を行ったコンピュータシステムから、通信媒体を通って、利用対象となるコンピュータシステムに伝達される。

【０００５】

【発明が解決しようとする課題】上述したように、従来は、コンピュータシステムの利用開始手続等に伴うユーザの認証を、利用対象となるコンピュータシステムが、当該コンピュータシステム自身が管理する利用者情報を基にして実施している。

【０００６】しかしながら、このようなシステムでは、通信媒体上を利用者の情報（ユーザ名やパスワード等）が第三者に判読可能な形で流れているため、安全上好ましくないという問題があった。また、ネットワーク上の各コンピュータ毎に管理する利用者情報が異なると、利

2

用者は、利用対象のコンピュータによって利用者識別子（パスワード）等を変えなければならず、操作性が損なわれるという問題もあった。

【０００７】本発明は、かかる従来の事情に対処してなされたもので、従来に較べて安全性の向上と、操作性の向上を図ることのできるユーザ認証システムを提供しようとするものである。

【０００８】

【課題を解決するための手段】すなわち、本発明は、複数のコンピュータシステムが通信媒体を介して接続され、これらのコンピュータシステムのファイルやＣＰＵを相互に利用可能に構成されたネットワークシステムのユーザ認証システムにおいて、前記ネットワークシステムに、前記各コンピュータシステムからのユーザ認証要求に応じて、ユーザ情報を格納する記憶手段を検索してユーザが登録されているか否かを判定し、ユーザが登録されている場合は、ユーザの正当性を制限時間付きで証明するチケットと前記記憶手段に格納されたパスワードとを暗号化して返送する認証用のコンピュータシステムを設けるとともに、前記各コンピュータシステムに、前記通信媒体上での前記ユーザ情報の交換を暗号化する暗号処理手段を設けたことを特徴とする。

【０００９】

【作用】上記構成の本発明のユーザ認証システムによれば、ネットワークにおけるユーザ情報を認証用のコンピュータシステムによって一元管理するので、パスワード等を統一することができ、従来に較べて操作性の向上を図ることができる。

【００１０】また、通信媒体には、第三者に判読可能な形でユーザ情報が流れることがなく、さらに、認証に使用されるチケットは時間制限が付いているので第三者に不当に使用される可能性も低減することができ、従来に較べて安全性の向上を図ることができる。

【００１１】

【実施例】以下、本発明の一実施例を、図面を参照して説明する。

【００１２】図１は本発明の一実施例の構成を示すものである。同図において、１は通信媒体であり、この通信媒体１を介して、複数のコンピュータシステム２、３、４、５が接続されている。

【００１３】上記各コンピュータシステムのうち、コンピュータシステム２は、ネットワーク上のユーザ情報を一括管理する認証サーバであり、ユーザ情報を格納するユーザ認証データベース２ａと、このユーザ認証データベース２ａを管理するデータベース管理部２ｂと、他のコンピュータシステム３、４、５からの認証要求を受けて認証サービスを行う認証サービス部２ｃと、サービス時にユーザの利用許可を判断する基となるチケットであって時間制限の付いたチケットを発行するチケット発行部２ｄと、情報の暗号化および復合を行う暗号処理部２

ｅと、通信媒体１を介して情報の送受信を行う通信制御部２ｆとを備えている。

【００１４】また、コンピュータシステム３、４、５は、ユーザが一般に利用するコンピュータであり、コンピュータシステム２に対して認証要求を行う認証要求部３ａ、４ａ、５ａと、他のコンピュータシステムに対してサービス要求を行うサービス要求部３ｂ、４ｂ、５ｂと、サービスを実行するサービス部３ｃ、４ｃ、５ｃと、前述した暗号処理を行う暗号処理部３ｄ、４ｄ、５ｄと、ユーザが入力を行うための入力部３ｅ、４ｅ、５ｅと、通信媒体１を介して情報の送受信を行う通信制御部３ｆ、４ｆ、５ｆとを備えている。

【００１５】ここで、コンピュータシステム３においてユーザが利用を開始し、コンピュータシステム４のサービスの利用を開始するまでの手続きを例にして、認証手順を説明する。

【００１６】まず、コンピュータシステム３の利用開始時における初期認証のユーザ認証手順について説明する。図２のフローチャートに示すように、まず、ユーザは、コンピュータシステム３の入力部３ｅから、認証要求部３ａに対して、ユーザ名を入力する（１００）。

【００１７】認証要求部３ａは、通信制御部３ｆにより、通信媒体１を介してこの入力されたユーザ名をコンピュータシステム（認証サーバ）２に送り、ユーザの初期チケットとユーザ認証データベース２ａに登録されている暗号化されたパスワードを要求する（１０１）。

【００１８】コンピュータシステム２においては、通信制御部２ｆによって受信したユーザ名を、認証サービス部２ｃに入力し、認証サービス部２ｃはユーザ名をデータベース管理部２ｂに送ってこのユーザ名がユーザ認証データベース２ａに登録されているか否かをチェックする（１０２）。

【００１９】そして、ユーザ名が登録されていれば、チケット発行部２ｄによって所定時間（例えば数時間乃至十数時間）の時間制限が付いた初期チケットを作成し（１０３）、この初期チケットと、ユーザ名に対応してユーザ認証データベース２ａに登録されているパスワードを、暗号処理部２ｅにおいて暗号化する（１０４）。ここで、初期チケットに時間制限を付けるのは、第三者による不正使用を防止するためである。すなわち、初期チケットに時間制限がないと、正当なユーザが認証を受け、初期チケットが発行されて、当該コンピュータシステムを使用した後、この初期チケットによって第三者が当該コンピュータシステムを不正使用する可能性があるからである。

【００２０】一方、ユーザがユーザ認証データベース２ａに登録されていない場合は、認証不可とし（１０５）、通信制御部２ｆを介して、これらの結果をコンピュータシステム３に返送する（１０６）。

【００２１】コンピュータシステム３では、通信制御部

３ｆにおいてこの結果を受信し、認証要求部３ａに入力する。認証要求部３ａでは、入力部３ｅからユーザにパスワードの入力を促し、ユーザがパスワードを入力すると（１０７）、暗号処理部３ｄにおいてコンピュータシステム２からの送信内容を復号し（１０８）、これらのパスワードが一致するか否かを判定する（１０９）。ここで、パスワードが一致すればコンピュータシステム３は利用可能となり、初期チケットは制限時間の間有効となる。また、パスワードが一致しなければ利用不可となる。

【００２２】なお、上記使用開始時におけるユーザ認証のプロトコルを、図５に示す。同図において、Ｃはコンピュータシステム３、ＡＳは認証サーバであるコンピュータシステム２を示している。

【００２３】次に、ユーザが、コンピュータシステム３からコンピュータシステム４のサービスを利用する場合について説明する。

【００２４】ユーザが、入力部３ｅからサービス要求部３ｂに、コンピュータシステム４のサービスを利用したい旨の入力を行うと、図３に示すように、まずサービス要求部３ｂは、サービス用の証明書（サービスチケット）があるか否かを調べ（２００）、サービスチケットが無い場合は、コンピュータシステム２に対してサービスチケットを要求する（２０１）。

【００２５】そして、サービスチケットがある場合は次に（サービスチケットがない場合はコンピュータシステム２からサービスチケットを受け取った後）、初期チケットが有効期限内か否かを調べ（２０２）、有効期限内であれば、暗号処理部３ｄでサービスチケットを暗号化し（２０３）、この暗号化したサービスチケットを通信制御部３ｆからコンピュータシステム４に送って、サービス要求を行う（２０４）。

【００２６】コンピュータシステム４では、通信制御部４ｅにおいて、上記サービス要求を受信し、このサービス要求をサービス部４ｃに入力する。サービス部４ｃでは、暗号処理部４ｄにおいて送られてきたサービスチケットを復号し（２０５）、正しいユーザであるか否かを確認（２０６）する。そして、正しいユーザである場合はサービスを受理する旨を返送してサービスを開始し、正しいユーザでない場合はサービスを拒否する旨を返送する。

【００２７】なお、上記サービス時におけるユーザ認証のプロトコルを、図６に示す。同図において、Ｃはコンピュータシステム３、ＡＳは認証サーバであるコンピュータシステム２、Ｓはサービスを行うコンピュータシステム４を示している。

【００２８】次に、上述したステップ２０１におけるサービスチケット要求、発行の処理を説明する。

【００２９】サービスチケットを有しない場合、図４に示すように、コンピュータシステム３では、まず、暗号

5

処理部３ｄにおいて、初期チケットと利用するコンピュータシステム名（コンピュータシステム４）を暗号化し（３００）、これらを通信制御部３ｆからコンピュータシステム２に送付して、サービスチケットの発行を要求をする（３０１）。

【００３０】コンピュータシステム２では、通信制御部２ｆにおいてこの要求を受信し、この要求は、認証サービス部２ｃに入力される。認証サービス部２ｃでは、暗号処理部２ｅによって送られてきたデータを復号し（３０２）、初期チケットが正しいか（時間切れでないか）否かを確認する（３０３）。

【００３１】そして、初期チケットが正しい場合は、チケット発行部２ｄにおいてサービスチケットを作成し（３０４）、このサービスチケットを暗号処理部２ｅによって暗号化して（３０５）、通信制御部２ｆからコンピュータシステム３に返送する。また、初期チケットが時間切れの場合等は、その旨をコンピュータシステム３に返送する（３０６）。

【００３２】コンピュータシステム３では、通信制御部３ｆによってサービスチケットを受信し、このサービスチケットを暗号処理部３ｄによって復号し、格納する（３０７）。

【００３３】このように、本実施例によれば、ネットワークにおけるユーザ情報を認証サーバであるコンピュータシステム２によって一元管理するので、パスワード等を統一することができ、従来に較べて操作性の向上を図ることができる。また、通信媒体１には、第三者に判読可能な形でユーザ情報が流れることがなく、さらに、認証に使用される初期チケット等は時間制限が付いている＊

6

＊ので第三者に不当に使用される可能性も低減することができ、従来に較べて安全性の向上を図ることができる。

【００３４】

【発明の効果】以上説明したように、本発明のユーザ認証システムによれば、従来に較べて安全性の向上と、操作性の向上を図ることができる。

【図面の簡単な説明】

【図１】本発明の一実施例の構成を示す図。

【図２】本発明の一実施例における使用開始時のユーザ認証の手順を示す図。

【図３】本発明の一実施例におけるサービス時のユーザ認証の手順を示す図。

【図４】本発明の一実施例におけるサービスチケット発行の手順を示す図。

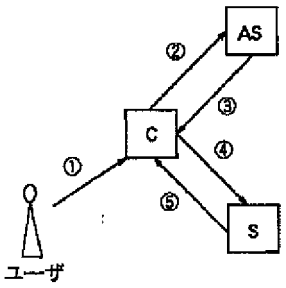
【図５】使用開始時におけるユーザ認証のプロトコルを示す図。

【図６】サービス時におけるユーザ認証のプロトコルを示す図。

【符号の説明】

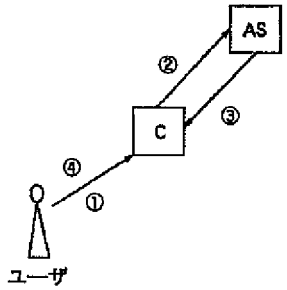
１　通信媒体
２　コンピュータシステム（認証用）
２ａ　ユーザ認証データベース
２ｂ　データベース管理部
２ｃ　認証サービス部
２ｄ　チケット発行部
２ｅ　暗号処理部
２ｆ　通信制御部
３、４、５　コンピュータシステム
３ｄ、４ｄ、５ｄ　暗号処理部

【図５】



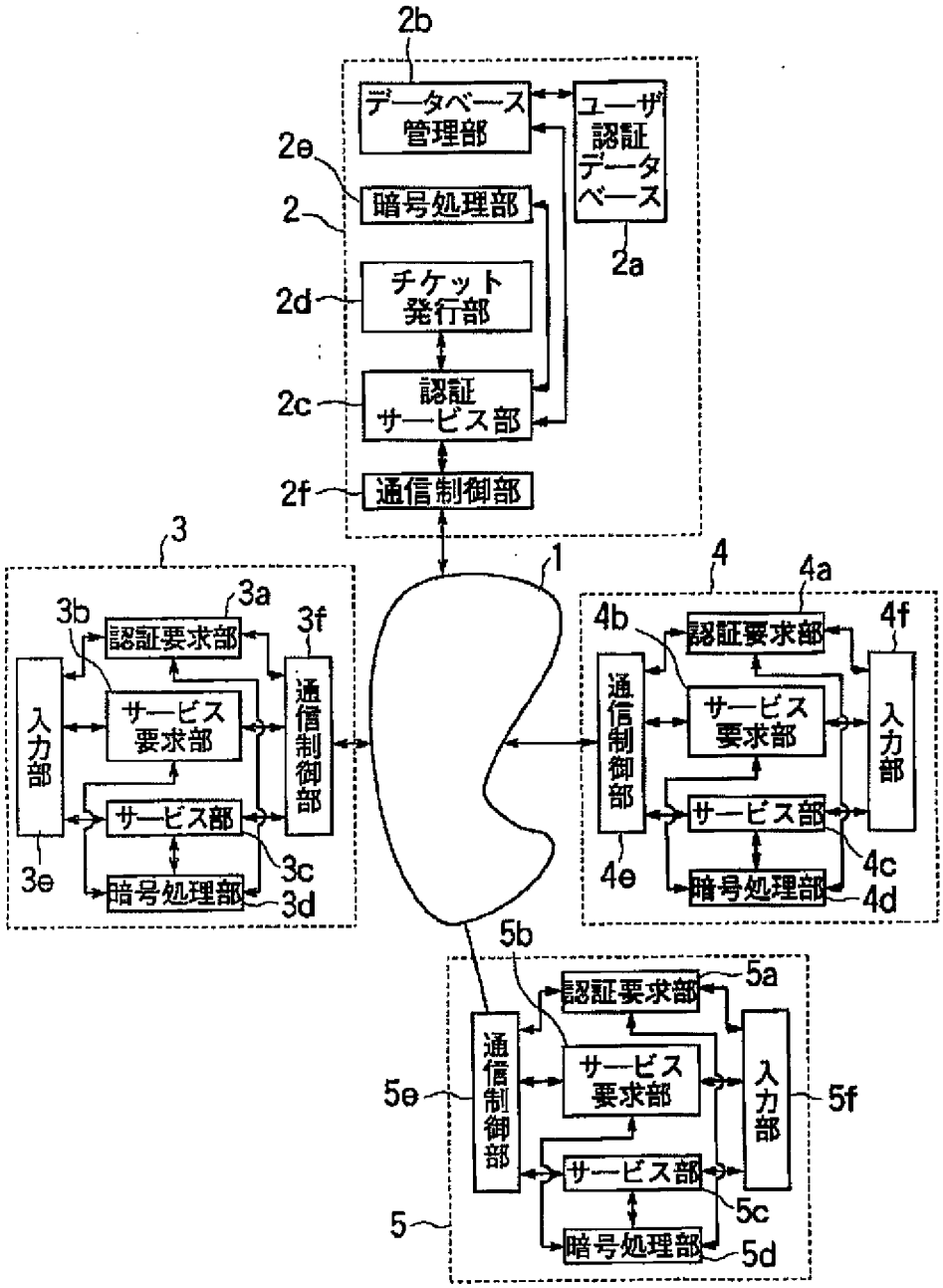
①サービス名
②初期チケットとサービスを受けたいマシン名
③サービスチケット
④サービスチケット
⑤利用の許可

【図６】

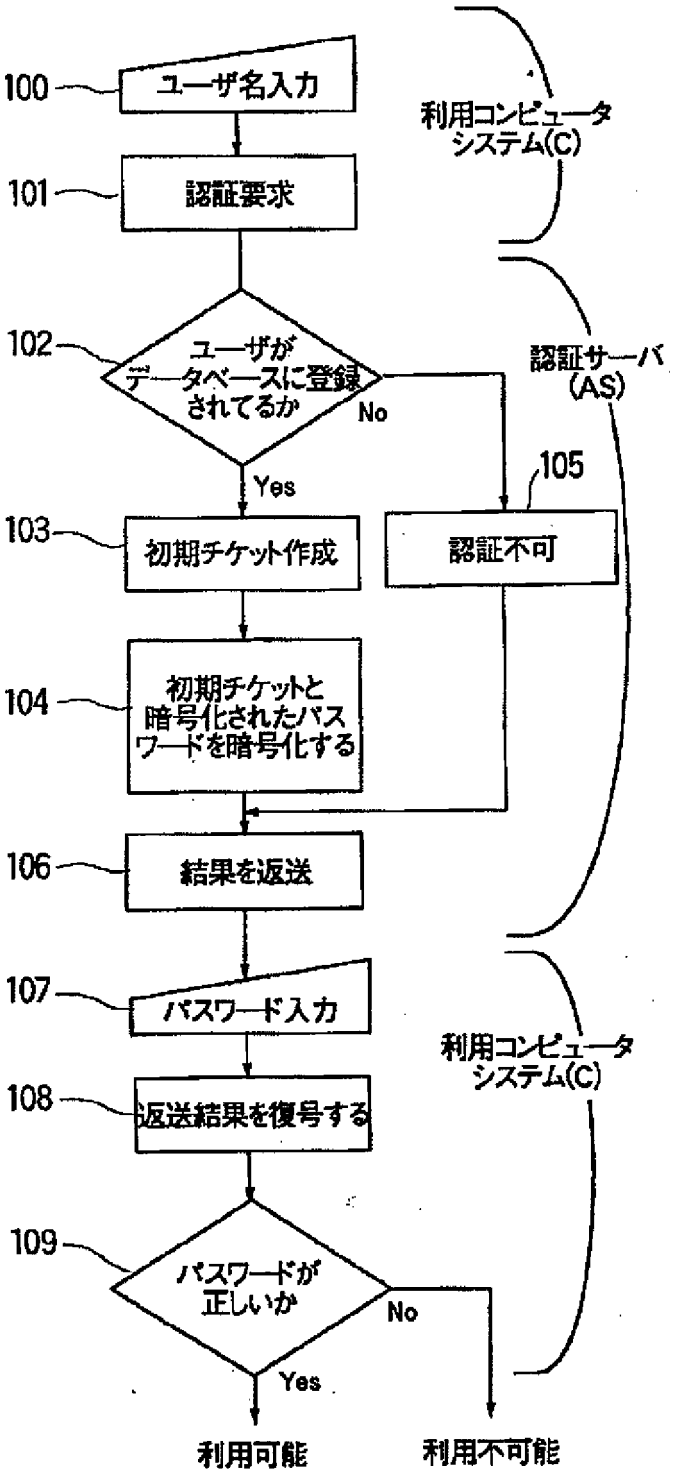


①ユーザ名
②ユーザ名と利用マシン名
③初期チケットと暗号化されたパスワード
④パスワード

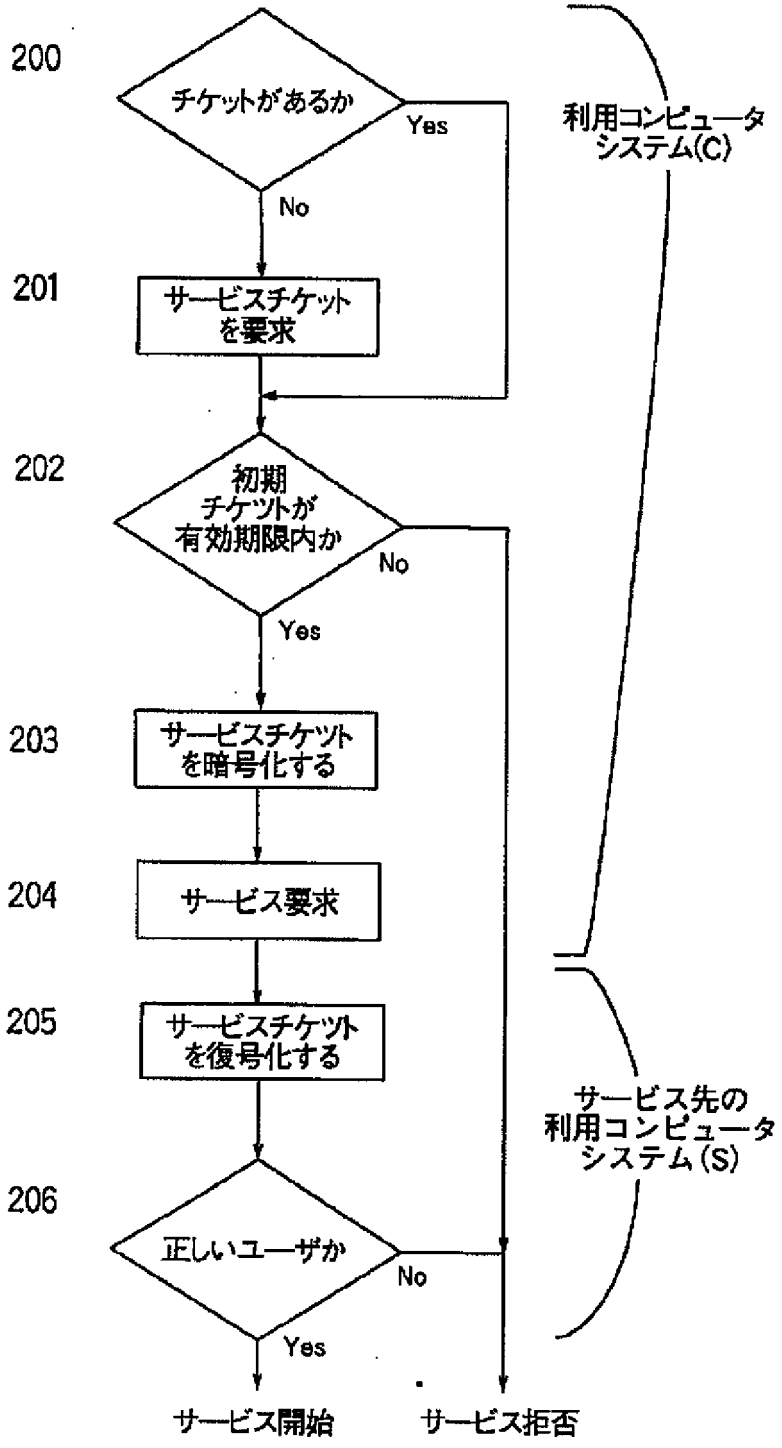
【図１】


2b
データベース管理部
ユーザ認証データベース
2a
2e
暗号処理部
2
2d
チケット発行部
2c
認証サービス部
2f
通信制御部
3
3b
3a
認証要求部
3f
入力部
サービス要求部
通信制御部
サービス部
3c
3e
暗号処理部
3d
1
4
4a
4b
認証要求部
4f
通信制御部
サービス要求部
入力部
サービス部
4c
4e
暗号処理部
4d
5b
5a
認証要求部
通信制御部
サービス要求部
入力部
5e
5f
サービス部
5c
5
暗号処理部
5d

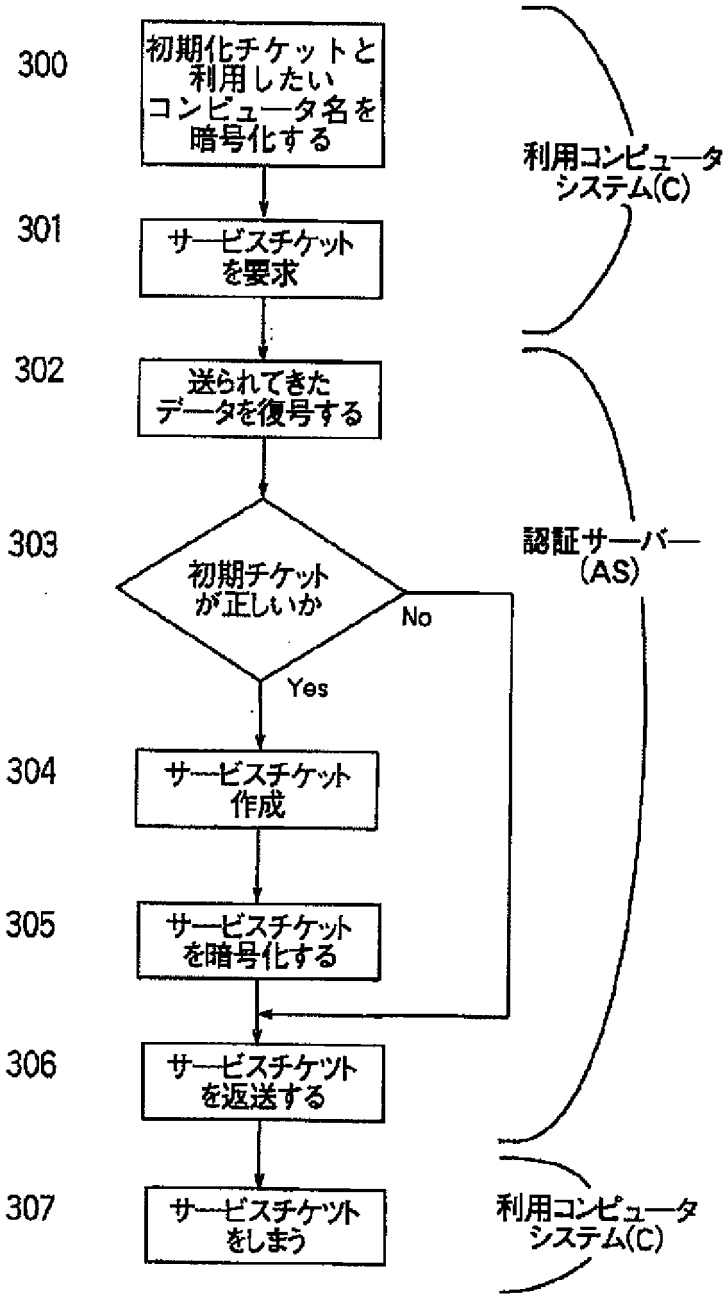
【図２】


100
ユーザ名入力
101
認証要求
利用コンピュータ
システム(C)
102
ユーザが
データベースに登録
されてるか
No
Yes
認証サーバ
(AS)
105
認証不可
103
初期チケット作成
104
初期チケットと
暗号化されたパス
ワードを暗号化する
106
結果を返送
107
パスワード入力
108
返送結果を復号する
109
パスワードが
正しいか
No
Yes
利用コンピュータ
システム(C)
利用可能
利用不可能

【図３】


200
チケットがあるか
Yes
No
利用コンピュータ
システム(C)
201
サービスチケット
を要求
202
初期
チケットが
有効期限内か
No
Yes
203
サービスチケット
を暗号化する
204
サービス要求
205
サービスチケット
を復号化する
サービス先の
利用コンピュータ
システム(S)
206
正しいユーザか
No
Yes
サービス開始
サービス拒否

【図４】


300
初期化チケットと利用したいコンピュータ名を暗号化する
301
サービスチケットを要求
302
送られてきたデータを復号する
303
初期チケットが正しいか
No
Yes
304
サービスチケット作成
305
サービスチケットを暗号化する
306
サービスチケットを返送する
307
サービスチケットをしまう
利用コンピュータシステム(C)
認証サーバー(AS)
利用コンピュータシステム(C)